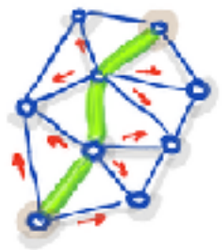
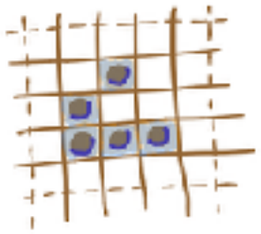
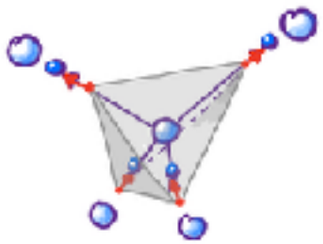
The Power of Massive Invariant Environments

methodological talk at EJC 2018







by Anatoly Ressin

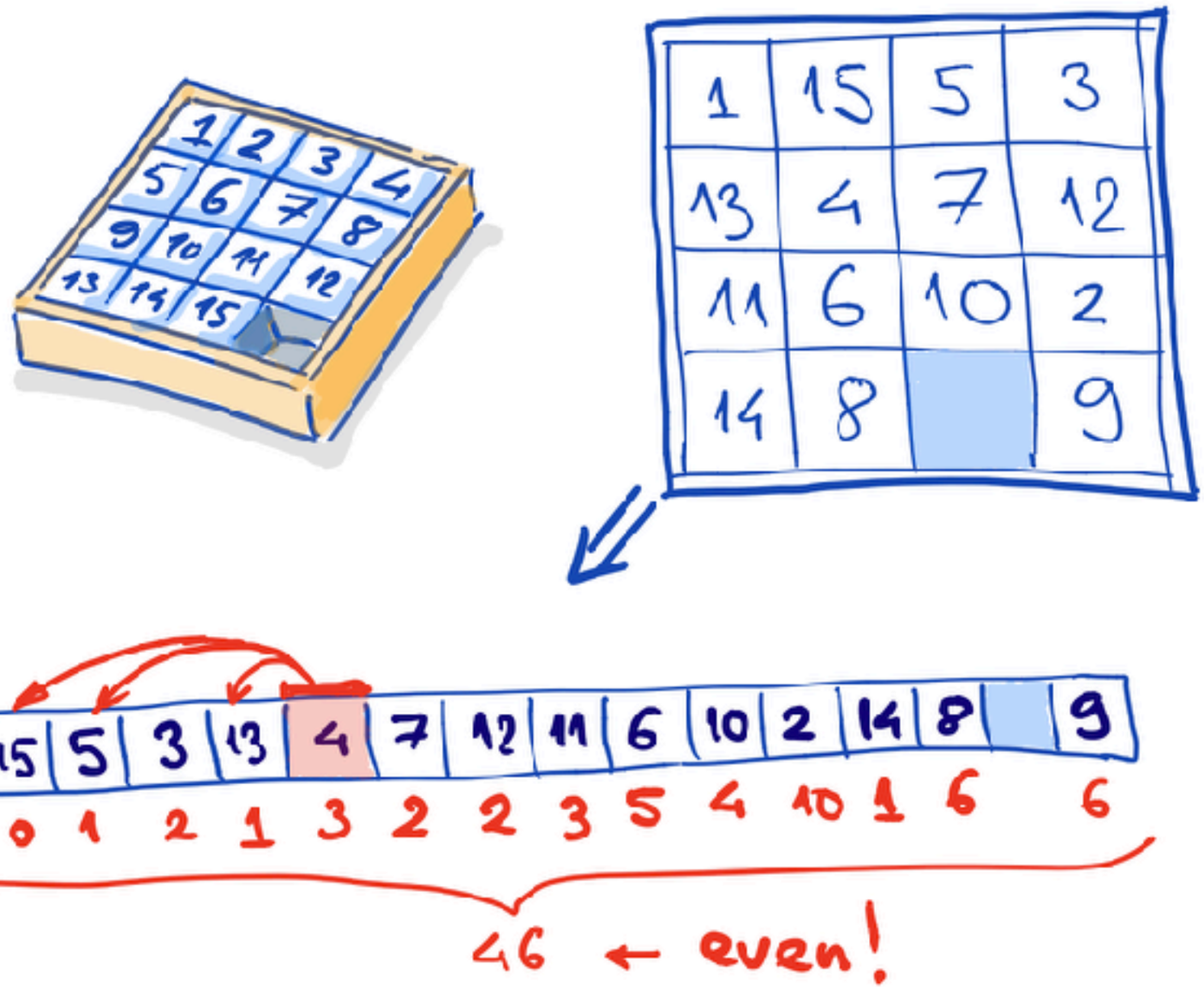
CEO, Blockchain Architect at Blockvis SIA
co-founder of Latvian Blockchain Association

Blockvis

Invariant

- A relation, function, quantity, or property which remains unchanged when a specified transformation is applied
- A powerful tool for analysis an proofs
- Almost always is constructed at meta-level

Example #1 (quantity)



Example #2 (static relation)

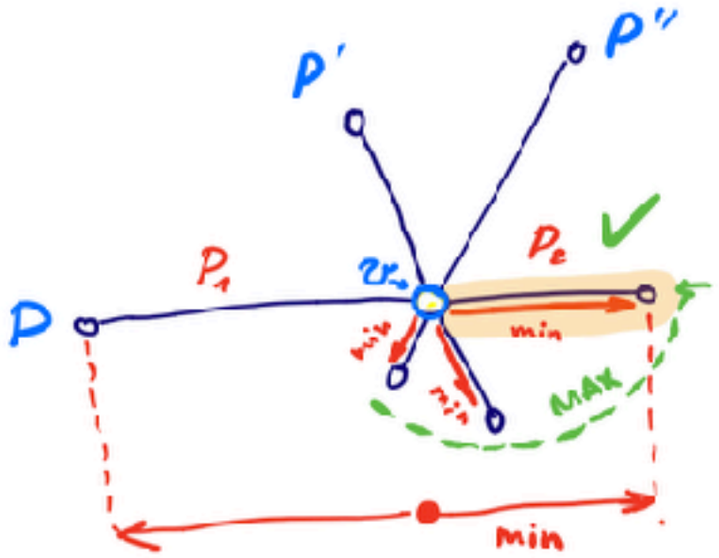
- Euclidean Distance (in space with euclidean metric) between two points is **always** shorter than any other path between the same points

- Could be used for A* search on graphs located in euclidean space

- Could be improved with another invariant: Triangle Inequality.

However, better relations exists

Carefuly crafted single property for every vertex called **Reach**



(Andrew V. Goldberg)
Reach for A*
Microsoft Research
2011

Consider a vertex v that splits a path P into P_1 and P_2

$reach_P(v) = \min(\ell(P_1), \ell(P_2))$

$reach(v) = \max_P(reach_P(v))$ over all shortest paths P through v

Ron Gutman, 2004

Massive Invariants

- Sometimes, to build a useful invariant we need to entangle the topology of the problem space with calculation for building a supporting data structure (eg. Reach property)

- When some slices of the problem space could be treated as co-existing points at given moment of time we can either

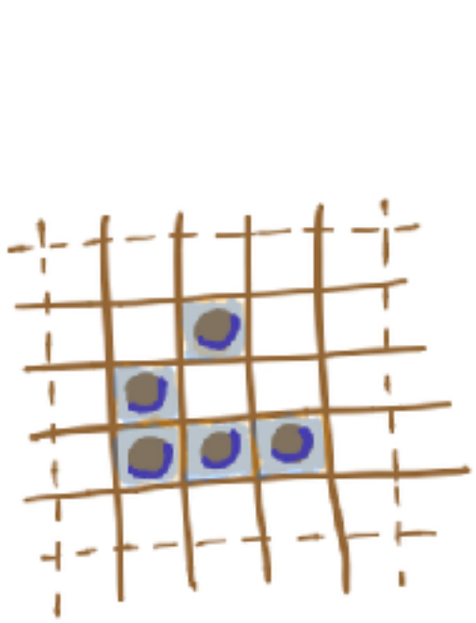
  - Define their passive invariant properties (quantities)

  - or define their invariant behaviour (transition functions)

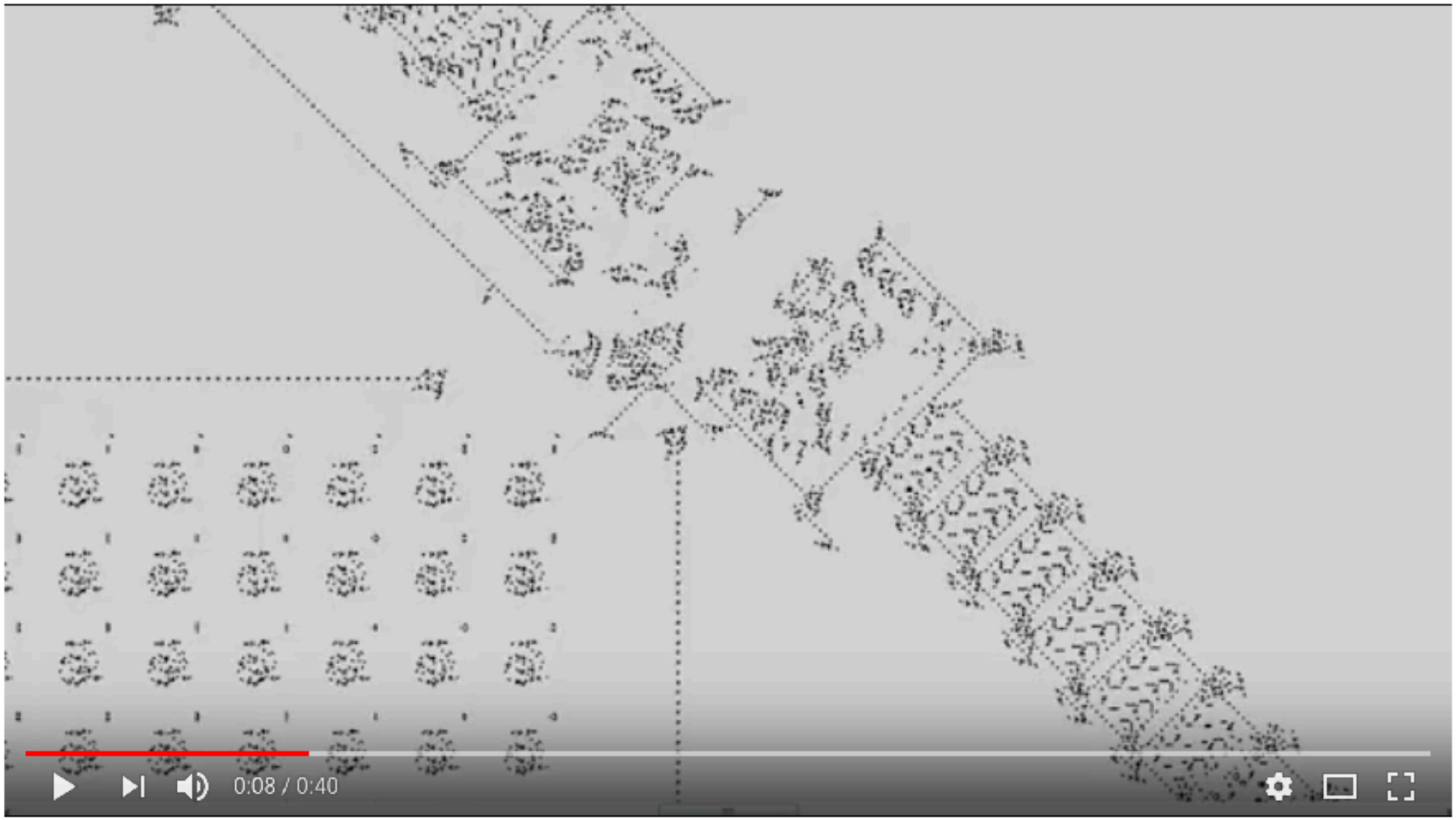
- Invariant that is defined for each co-existing point of the space we call here a **Massive Invariant**

Wonders of Massive Invariants

Cellular Automata: Conway's Game of Life



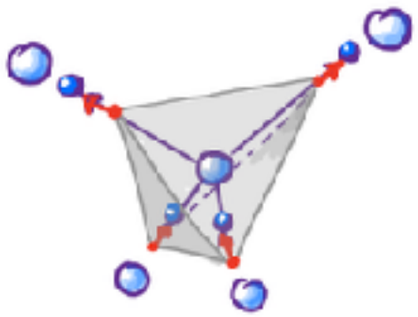
Game of Life: Universal Turing Machine



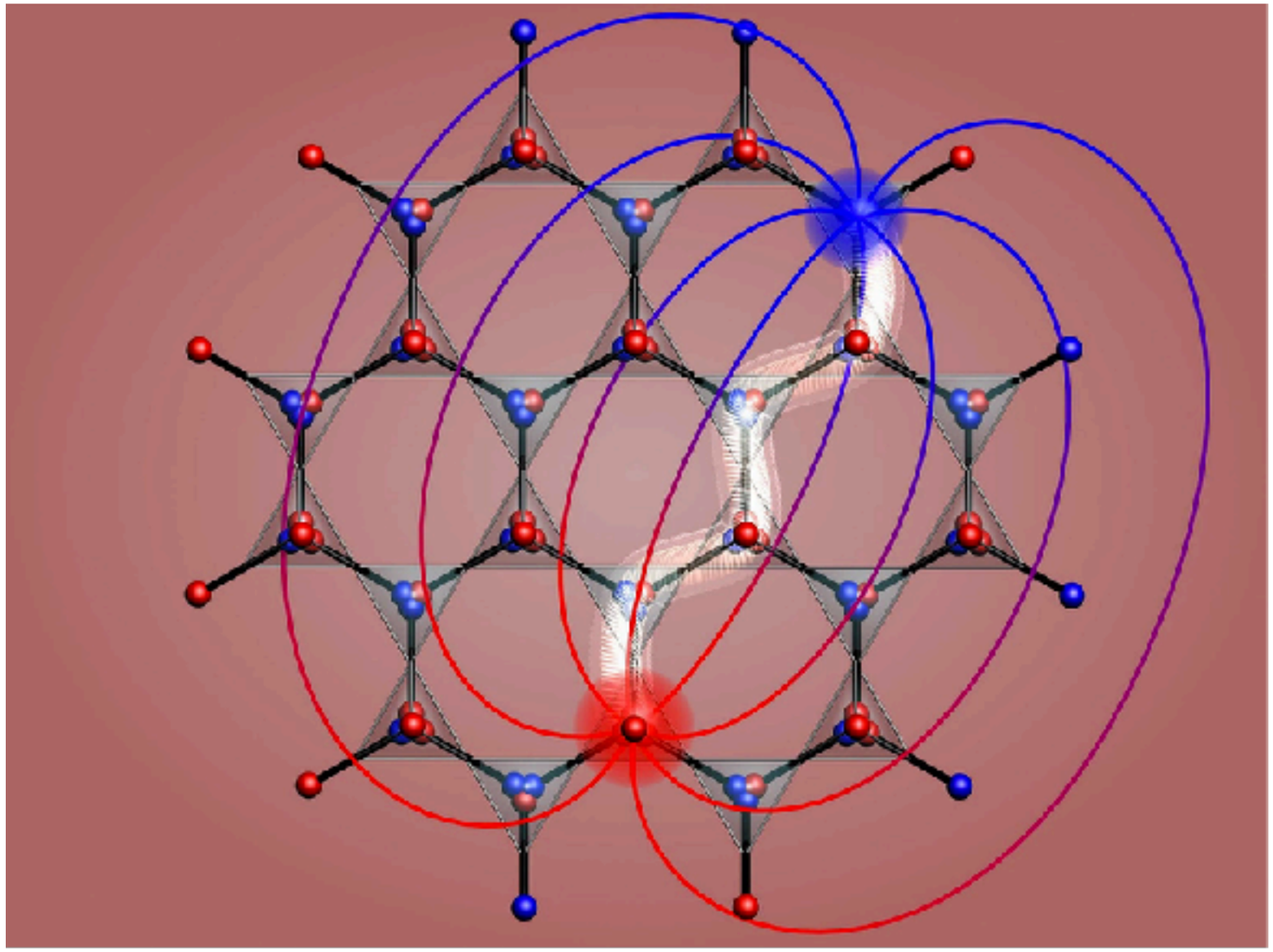
Game of Life - Universal Turing Machine https://www.youtube.com/watch?v=My8AsV7bA94

Physical Example

Modeling Magnetic Monopole in the environment of $Dy_2Ti_2O_7$



Magnetic moments of the molecule organised in a way that allows to form a model of Magnetic monopole



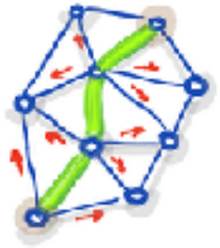
Blockchain Example

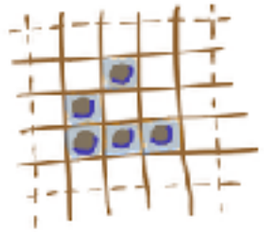
- One of the most wonderful from practical massive invariant: **Consensus (EG: BFT)**

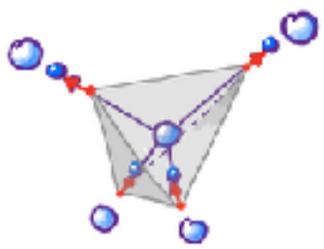
- Every **Honest** Node Executes the same protocol

- If there is majority of Honest Nodes every Honest Node will see the same state eventually

Conclusion

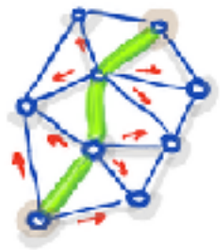


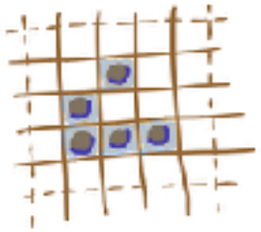


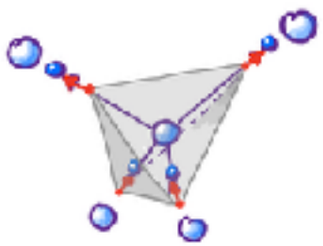


Sometimes you need to represent your problem space as the space where some massive invariant is constructible and it will give you an more power than you can expect.

Thank you for the attention!







bitcoin

by Anatoly Ressin

CEO, Blockchain Architect at Blockvis SIA
co-founder of Latvian Blockchain Association

Blockvis